PATENT ABSTRACTS OF JAPAN

(11)Publication number : 03-128541
(43)Date of publication of application : 31.05.1991

(51)Int.Cl. H04L 9/06
G09C 1/00
H04L 9/14

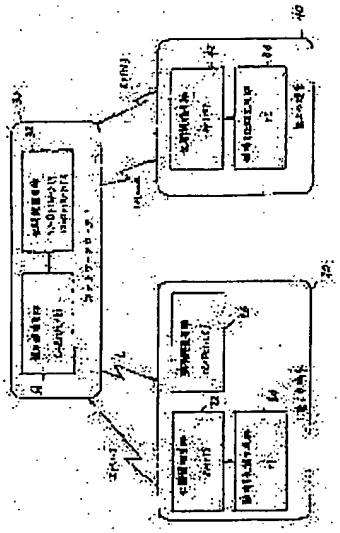
(21)Application number : 02-209990
(22)Date of filing : 07.08.1990

(71)Applicant : MATSUSHITA ELECTRIC IND CO LTD
(72)Inventor : TATEBAYASHI MAKOTO
MATSUZAKI NATSUME
DEBITSUDO BII NIYUUMAN JIYUNIA

(30)Priority
Priority number : 89 390048 Priority date : 07.08.1989 Priority country : US

(54) SYSTEM AND METHOD FOR CIPHER COMMUNICATION

(57)Abstract:
PURPOSE: To safely distribute a secret key while transmitting public information through a network center between plural terminals each other by converting a key ciphering key and structure data to a cipher sentence by using public cipher key algorithm and transmitting the cipher sentence to a communication path.
CONSTITUTION: In a first open key cipher part 22, a key ciphering key r1 generated by a key ciphering key generation part 24 is ciphered to the first cipher sentence by using the public key cipher algorithm. The first public cipher part 22 transmits this sentence to the communication path. In a second terminal 40, a second key ciphering key signal r2 is generated by a second key ciphering key generation part 44 and a second key ciphering key r2 is ciphered to the second cipher sentence and transmitted to a network center 30. A public key decoding part 32 in the network center 30 decodes the first and second cipher sentences by using public key decoding algorithm. As a result, the network center 30 obtains the first and second key ciphering keys r1 and r2.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

⑲日本国特許庁(JP)　⑪特許出願公開

⑫公開特許公報(A)　平3-128541

⑤Int.Cl.⁵	識別記号	庁内整理番号	㊸公開　平成3年(1991)5月31日
H 04 L 9/06			
G 09 C 1/00		7343-5B	
H 04 L 9/14			
		6914-5K　H 04 L 9/02　Z	

審査請求　未請求　請求項の数 35　(全17頁)

㊹発明の名称　暗号通信システムと暗号通信方法

㉑特　願　平2-209990

㉒出　願　平2(1990)8月7日

優先権主張　㉜1989年8月7日㉝米国(US)㉛390,048

㉗発明者　館林　誠　大阪府門真市大字門真1006番地　松下電器産業株式会社内

㉗発明者　松崎　なつめ　大阪府門真市大字門真1006番地　松下電器産業株式会社内

㉗発明者　デビッド　ビー　ニューマン　ジュニア　アメリカ合衆国メリーランド州　ラ　プラタ　センテニアル　スクエア

㉑出願人　松下電器産業株式会社　大阪府門真市大字門真1006番地

㉔代理人　弁理士　小鍜治　明　外2名

明細書

1.発明の名称

暗号通信システムと暗号通信方法

2.特許請求の範囲

(1)第1、第2の端末と通信路とネットワークセンターからなるシステムであって、

前記第1の端末にあり、第1の鍵暗号化鍵を生成する第1の生成手段と、

前記第1の端末にあり、第1の構造化データを生成する第1の構造化手段と、

前記第1の端末にあり、前記第1の生成手段と前記第1の構造化手段と前記通信路に接続し、公開鍵暗号アルゴリズムを用いて第1の鍵暗号化鍵と第1の構造化データを第1の暗号文に変換し、この第1の暗号文を前記通信路に送信する第1の暗号化手段と、

前記ネットワークセンターにあり、第1の暗号文を受け取ると、要求信号を生成して前記通信路に送信する手段と、

前記第2の端末にあり、要求信号を受け取ると、第2の鍵暗号化鍵を生成する第2の生成手段と、

前記第2の端末にあり、第2の構造化データを生成する第2の構造化手段と、

前記第2の端末にあり、前記第2の生成手段と前記第2の構造化手段と前記通信路に接続し、公開鍵暗号アルゴリズムを用いて第2の鍵暗号化鍵と第2の構造化データを第2の暗号文に変換し、その第2の暗号文を前記通信路に送信する第2の暗号化手段と、

前記ネットワークセンターにあり、前記通信路と接続し、公開鍵復号アルゴリズムを用いて第1の暗号文と第2の暗号文を復号し、これにより第1の鍵暗号化鍵と第1の構造化データと第2の鍵暗号化鍵と第2の構造化データを得る第1の復号手段と、

前記ネットワークセンターにあり、前記第1の復号手段に接続し、第1の構造化データと第2の構造化データの正当性を確認し、確認信号を生成する手段と、

前記ネットワークセンターにあり、前記第1の

復号手段と前記確認手段と前記通信路に接続し、確認信号を受け取ると、慣用鍵暗号アルゴリズムを用いて第1の鍵暗号化鍵と第2の鍵暗号化鍵を第3の暗号文に変換し、この第3の暗号文を前記通信路に送信する第3の暗号手段と、

前記第1の端末にあり、前記通信路と接続し、慣用鍵復号アルゴリズムと第1の鍵暗号化鍵を用いて、第3の暗号文を復号し、これにより第2の鍵暗号化鍵を得る第2の復号手段と

を備えた暗号通信システム。

(2)特許請求の範囲第1項において、

前記第1の構造化手段が第1のタイムスタンプを含む第1の構造化データを生成し、

前記確認手段が第1のタイムスタンプを確認する暗号通信システム。

(3)特許請求の範囲第1項において、

前記第1の構造化手段が第1の識別情報を含む第1の構造化データを生成し、

前記確認手段が第1の識別情報を確認する暗号通信システム。

(4)特許請求の範囲第1項において、

前記第2の構造化手段が第2のタイムスタンプを含む第2の構造化データを生成し、

前記確認手段が第2のタイムスタンプを確認する暗号通信システム。

(5)特許請求の範囲第1項において、

前記第2の構造化手段が第2の識別情報を含む第2の構造化データを生成し、

前記確認手段が第2の識別情報を確認する暗号通信システム。

(6)特許請求の範囲第1項において、

前記第1の暗号化手段が第1の鍵暗号化鍵と構造化データのべき乗剰余演算手段を含んでいる暗号通信システム。

(7)特許請求の範囲第1項において、

前記第2の暗号化手段が第2の鍵暗号化鍵と構造化データのべき乗剰余演算手段を含んでいる暗号通信システム。

(8)第1、第2の端末と通信路とネットワークセンターからなるシステムであって、

前記第1の端末にあり、第1の鍵暗号化鍵を生成する第1の生成手段と、

前記第1の端末にあり、前記第1の生成手段と前記通信路に接続し、公開鍵暗号アルゴリズムを用いて第1の鍵暗号化鍵を第1の暗号文に変換し、その第1の暗号文を前記通信路に送信する第1の暗号化手段と、

前記第2の端末にあり、第2の鍵暗号化鍵を生成する第2の生成手段と、

前記第2の端末にあり、前記第2の生成手段と前記通信路に接続し、公開鍵暗号アルゴリズムを用いて第2の鍵暗号化鍵を第2の暗号文に変換し、その第2の暗号文を前記通信路に送信する第2の暗号化手段と、

前記ネットワークセンターにあり、前記通信路と接続し、公開鍵復号アルゴリズムを用いて第1の暗号文と第2の暗号文を復号し、これにより第1の鍵暗号化鍵と第2の鍵暗号化鍵を得る第1の復号手段と、

前記ネットワークセンターにあり、前記第1の復号手段と前記通信路に接続し、慣用鍵暗号アルゴリズムを用いて第1の鍵暗号化鍵と第2の鍵暗号化鍵を第3の暗号文に変換し、その第3の暗号文を前記通信路に送信する第3の暗号手段と、

前記第1の端末にあり、前記通信路と接続し、慣用鍵復号アルゴリズムと第1の鍵暗号化鍵を用いて、第3の暗号文を復号し、これにより第2の鍵暗号化鍵を得る第2の復号手段と

を備えた暗号通信システム。

(9)特許請求の範囲第8項において、

前記第1の端末にあり、第1の構造化データを生成する第1の構造化手段を備え、

前記第1の暗号化手段は前記第1の構造化手段に接続し、公開鍵暗号アルゴリズムを用いて第1の鍵暗号化鍵と第1の構造化データを第1の暗号文に変換する暗号通信システム。

(10)特許請求の範囲第8項において、

前記第2の端末にあり、第2の構造化データを生成する第2の構造化手段を備え、

前記第2の暗号化手段は前記第2の構造化手段

に接続し、公開鍵暗号アルゴリズムを用いて第2の鍵暗号化鍵と第2の構造化データを第2の暗号文に変換する暗号通信システム。

(11) 特許請求の範囲第9項において、

前記ネットワークセンターにあり、前記第1の復号手段に接続し、第1の構造化データの正当性を確認して確認信号を生成する手段を備え、

前記第3の暗号手段は前記確認手段と接続し、確認信号を受け取ると、慣用鍵暗号アルゴリズムを用いて第1の鍵暗号化鍵と第2の鍵暗号化鍵を第3の暗号文に変換し、その第3の暗号文を前記通信路に送信する暗号通信システム。

(12) 特許請求の範囲第10項において、

前記ネットワークセンターにあり前記第1の復号手段に接続し、第2の構造化データの正当性を確認して確認信号を生成する手段を備え、

前記第3の暗号手段は前記確認手段と接続し、確認信号を受け取ると、慣用鍵暗号アルゴリズムを用いて第1の鍵暗号化鍵と第2の鍵暗号化鍵を第3の暗号文に変換し、その第3の暗号文を前記通信路に送信する暗号通信システム。

(13) 特許請求の範囲第8項において、

前記ネットワークセンターにあり、第1の暗号文を受け取ると、要求信号を生成して前記通信路に送信する手段を備え、

前記第2の生成手段は前記要求信号を受け取ると、第2の鍵暗号鍵を生成する暗号通信システム。

(14) 特許請求の範囲第8項において、

前記第1の暗号化手段が第1の鍵暗号化鍵のべき乗剰余手段を含んで、第1の暗号文を生成する暗号通信システム。

(15) 特許請求の範囲第8項において、

前記第2の暗号化手段が第2の鍵暗号化鍵のべき乗剰余手段を含んで、第2の暗号文を生成する暗号通信システム。

(16) 第1、第2の端末と通信路とネットワークセンターを用いた暗号通信方法であって、

前記第1の端末において、第1の鍵暗号化鍵と第1の構造化データを生成するステップと、

前記第1の端末において、公開鍵暗号アルゴリズムを用いて第1の鍵暗号化鍵と第1の構造化データを第1の暗号文に変換するステップと、

この第1の暗号文を前記通信路に送信するステップと、

前記ネットワークセンターにおいて、第1の暗号文を受け取ると、要求信号を生成しこの要求信号を前記ネットワークセンターから前記通信路に送信するステップと、

前記第2の端末において、要求信号を受け取ると、第2の鍵暗号化鍵を生成するステップと、

前記第2の端末において、第2の構造化データを生成するステップと、

前記第2の端末において、公開鍵暗号アルゴリズムを用いて第2の鍵暗号化鍵と第2の構造化データを第2の暗号文に変換し、この第2の暗号文を前記通信路に送信するステップと、

前記ネットワークセンターにおいて、公開鍵復号アルゴリズムを用いて第1の暗号文と第2の暗号文を復号して、これにより第1の鍵暗号化鍵と第1の構造化データと第2の鍵暗号化鍵と第2の構造化データを得するステップと、

前記ネットワークセンターにおいて、第1の構造化データと第2の構造化データの正当性を確認し、確認信号を生成するステップと、

前記ネットワークセンターにおいて、確認信号を受け取ると、慣用鍵暗号アルゴリズムを用いて第1の鍵暗号化鍵と第2の鍵暗号化鍵を第3の暗号文に変換し、この第3の暗号文を前記通信路に送信するステップと、

前記第1の端末において、慣用鍵復号アルゴリズムと第1の鍵暗号化鍵を用いて、第3の暗号文を復号し、これにより第2の鍵暗号化鍵を得るステップからなる暗号通信方法。

(17) 特許請求の範囲第16項において、

前記第1の端末の生成ステップで、第1のタイムスタンプを含む第1の構造化データを生成し、前記ネットワークセンターの確認ステップで第1のタイムスタンプを確認する暗号通信方法。

(18) 特許請求の範囲第16項において、

前記第1の端末の生成ステップで、第1の識別

情報を含む第1の構造化データを生成し、
前記ネットワークセンターの確認ステップで第1の識別情報を確認する暗号通信方法。
(19) 特許請求の範囲第16項において、
前記第2の端末の生成ステップで第2のタイムスタンプを含む第2の構造化データを生成し、
前記前記ネットワークセンターの確認ステップで第2のタイムスタンプを確認する暗号通信方法。
(20) 特許請求の範囲第16項において、
前記第2の端末の生成ステップで第2の識別情報を含む第2の構造化データを生成し、
前記前記ネットワークセンターの確認ステップで第2の識別情報を確認する暗号通信方法。
(21) 特許請求の範囲第16項において、
前記第1の端末の変換ステップが、第1の鍵暗号化鍵と構造化データのべき乗剰余演算を含む暗号通信方法。
(22) 特許請求の範囲第16項において、
前記第2の端末の変換ステップが、第2の鍵暗号化鍵と構造化データのべき乗剰余演算を含む暗号通信方法。
(23) 第1の鍵暗号化鍵を生成するステップと、
公開鍵暗号アルゴリズムを用いて、第1の鍵暗号化鍵を第1の暗号文に変換するステップと、
第2の鍵暗号化鍵を生成するステップと、
公開鍵暗号アルゴリズムを用いて、第2の鍵暗号化鍵を第2の暗号文に変換するステップと
公開鍵復号アルゴリズムを用いて、第1の暗号文と第2の暗号文を復号し、これにより第1の鍵暗号化鍵と第2の鍵暗号化鍵を得るステップと、
慣用鍵暗号アルゴリズムを用いて、第1の鍵暗号化鍵と第2の鍵暗号化鍵を第3の暗号文に変換するステップと、
慣用鍵復号アルゴリズムと第1の鍵暗号化鍵を用いて、第3の暗号文を復号し、これにより第2の鍵暗号化鍵を得るステップからなる暗号通信方法。
(24) 特許請求の範囲第23項において、
第1の構造化データを生成するステップと、
第1の鍵暗号化鍵と第1の構造化データを第1の暗号文に変換するステップを有する暗号通信方法。
(25) 特許請求の範囲第23項において、
第2の構造化データを生成するステップと、
第2の鍵暗号化鍵と第2の構造化データを第2の暗号文に変換するステップを有する暗号通信方法。
(26) 特許請求の範囲第24項において、
第1の構造化データの正当性を確認して確認信号を生成するステップと、
確認信号を受けると慣用鍵暗号アルゴリズムを用いて第1の鍵暗号化鍵と第2の鍵暗号化鍵を第3の暗号文に変換するステップを有する暗号通信方法。
(27) 特許請求の範囲第25項において、
第2の構造化データの正当性を確認して確認信号を生成するステップと、
確認信号を受けると慣用鍵暗号アルゴリズムを用いて第1の鍵暗号化鍵と第2の鍵暗号化鍵とを暗号化して第3の暗号文を得るステップを有する暗号通信方法。
(28) 特許請求の範囲第23項において、
要求信号を生成するステップと、
要求信号を受けると第2の鍵暗号化鍵を生成するステップを有する暗号通信方法。
(29) 特許請求の範囲第23項において、
公開鍵暗号アルゴリズムを用いた変換ステップが、第1の鍵暗号化鍵のべき乗剰余演算を含む暗号通信方法。
(30) 特許請求の範囲第23項において、
公開鍵暗号アルゴリズムを用いた変換ステップが、第2の鍵暗号化鍵のべき乗剰余演算を含む暗号通信方法。
(31) 第1、第2の端末を含みネットワークセンターを用いた暗号通信方法であって、
前記ネットワークセンターの公開鍵eと法nを用いて、第1の鍵暗号化鍵r1を第1の暗号文 $r1^e \bmod n$ に変換するステップと、
前記ネットワークセンターの秘密鍵dを用いて、$(r1^e \bmod n)^d \bmod n$ で第1の暗号文を

復号するステップと、

前記ネットワークセンターの公開鍵eと法nを用いて、第2の鍵暗号化鍵r2を第2の暗号文r2^e modulo n に変換するステップと、

前記ネットワークセンターの秘密鍵dを用いて、(r2^e modulo n)^d modulo n で第2の暗号文を復号するステップと、

第2の鍵暗号化鍵と第1の鍵暗号化鍵を暗号化して第3の暗号文を生成するステップと、

第1の鍵暗号化鍵を用いて、第3の暗号文を復号するステップからなる暗号通信方法。

(32)第1の鍵暗号化鍵を生成するステップと、

公開鍵暗号アルゴリズムを用いて第1の鍵暗号化鍵を第1の暗号文に変換するステップと、

第2の鍵暗号鍵を生成するステップと、

公開鍵暗号アルゴリズムを用いて第2の鍵暗号化鍵を第2の暗号文に変換するステップと、

公開鍵復号アルゴリズムを用いて第1の暗号文と第2の暗号文を復号し、第1の鍵暗号化鍵と第2の鍵暗号化鍵を得るステップと、

第2の鍵暗号化鍵と第1の鍵暗号化鍵を暗号化して第3の暗号文を生成するステップと、

第2の鍵暗号化鍵を用いて第3の暗号文を復号するステップからなる暗号通信方法。

(34)特許請求の範囲第31項において、

第3の鍵暗号化鍵を生成するステップと、

公開鍵暗号アルゴリズムを用いて第3の鍵暗号化鍵を第4の暗号文に変換するステップと、

公開鍵復号アルゴリズムを用いて第4の暗号文を復号し、第3の鍵暗号化鍵を得るステップと、

慣用鍵暗号アルゴリズムを用いて第1の鍵暗号化鍵と第3の鍵暗号化鍵を第5の暗号文に変換するステップと、

慣用鍵復号アルゴリズムと第1の鍵暗号化鍵を用いて、第5の暗号文を復号し第3の鍵暗号化鍵を得るステップを有する暗号通信方法。

(35)特許請求の範囲第16項において、

第3の端末において要求信号を受け取ると、第3の鍵暗号化鍵と第3の構造化データを生成するステップと、

慣用鍵暗号アルゴリズムを用いて第1の鍵暗号化鍵と第2の鍵暗号化鍵を第3の暗号文に変換するステップと、

慣用鍵復号アルゴリズムと第2の鍵暗号化鍵を用いて、第3の暗号文を復号し、第1の鍵暗号化鍵を得るステップからなる暗号通信方法。

(33)第1、第2の端末を含み、ネットワークセンターを用いた暗号通信方法であって、

前記ネットワークセンターの公開鍵eと法nを用いて、第1の鍵暗号化鍵r1を第1の暗号文r1^e modulo n に変換するステップと、

前記ネットワークセンターの秘密鍵dを用いて、(r1^e modulo n)^d modulo n で第1の暗号文を復号するステップと、

前記ネットワークセンターの公開鍵eと法nを用いて、第2の鍵暗号化鍵r2を第2の暗号文r2^e modulo n に変換するステップと、

前記ネットワークセンターの秘密鍵dを用いて、(r2^e modulo n)^d modulo n で第2の暗号文を復号するステップと、

前記第3の端末において、公開鍵暗号アルゴリズムを用いて第3の鍵暗号化鍵と第3の構造化データを第4の暗号文に変換するステップと、

この第4の暗号文を通信路に送信するステップと、

前記ネットワークセンターにおいて、公開鍵復号アルゴリズムを用いて第4の暗号文を復号し、第3の鍵暗号化鍵と第3の構造化データを得るステップと、

前記ネットワークセンターにおいて、第3の構造化データの正当性を確認し、確認信号を生成するステップと、

前記ネットワークセンターにおいて、慣用鍵暗号アルゴリズムを用いて第2の鍵暗号化鍵と第3の鍵暗号化鍵を第5の暗号文に変換するステップと、この第5の暗号文を前記通信路に送信するステップと、

前記第3の端末において、慣用鍵復号アルゴリズムと第3の鍵暗号化鍵を用いて第5の暗号文を復号し、第2の鍵暗号化鍵を得るステップからな

る暗号通信方法。

3.発明の詳細な説明

産業上の利用分野

本発明は、ディジタル移動通信システム、特に複数の端末がネットワークセンターを通じて安全に暗号鍵を配送するプロトコルの実現方法とシステムに関する。

従来の技術

近年の通信技術（パーソナルコンピュータ、LAN、分散データベース、ポケットベル、人工衛星を用いた電子会議、電子メール、電子現金取引をふくむ）の進展により、そこで扱われる情報の価値が認識されてきている。それにともない、傍受に対する通信リンクの弱点と、データベースの利己的利用や改竄に対する脆弱さがますます意識されてきている。これらのことにより、盗聴や改竄に対して安全な通信を提供するテクニックの適用範囲が拡大してきている。

安全な通信ネットワークのユーザとしてはまず銀行が上げられる。銀行では、電子的に輸送される資金が、途中で改竄されずに正しく送られることが必要である（つまりメッセージ認証問題）。同様に、コンピュータネットワークを用いて操作を行なう証券会社では、株式の売買が正規の人との間で確実に行なわれることが必要である。

これらのことより、送受信者はますます通信におけるプライバシーや安全性の問題に意識を向けるようになってきている。盗聴とデータの偽造に対して安全性を提供する技術的方法の1つが暗号である。一般的に鍵の配送には、慣用鍵暗号を用いた方法と公開鍵暗号を用いた方法の2つがある。

慣用鍵暗号を用いて安全な通信を行なうためには送受信者は同じ鍵をもたなければならない。送信者は暗号鍵を用いてメッセージに鍵をかけ、受信者はこのメッセージにかけた鍵を開けるために送信者と同じ鍵をもたなくてはならない。大規模ネットワークにおける鍵配送について考える。

大規模ネットワークにおいてはたくさんの端末間で鍵を配送することが必要になる。ネットワーク上のすべての端末が同じ鍵を用いている場合、もしただ1つの端末から鍵が求められると、ネットワーク自身が危険になる。

そこで、各端末対ごとに鍵を違える必要がある。ところがそうすると、n個の端末に対してn(n-1)/2個の鍵が必要になり、鍵管理が大変である。また、第4図に示すとおり、暗号化鍵EAを用いて生成した暗号文Cをもとのメッセージ M に直すには、秘密の通信路を用いて復号鍵を受信者に送信することが必要である。この秘密の通信路は、暗号化の必要不可欠な要素であるセッション鍵の生成、格納、配送、消去、記録にも必要である。従って、秘密の通信路をネットワークの各端末間に張りめぐらせることが必要である。

一方、公開鍵暗号方式は不特定多数の端末と暗号通信を行なうための技術である。ハードウェアの低価格化にともない、その実現も容易になってきている。特にコンピュータ通信ネットワークにおいて、公開鍵暗号方式は端末間の鍵配送、そして通信のプライバシーやメッセージの正当性を保証するための、慣用鍵暗号方式と比べても比較的安価な暗号方式である。

（公開鍵暗号方式）

公開鍵暗号方式には一方向性落し戸関数が用いられている。まず、この一方向性関数について説明する。一方向性関数は、その関数の計算は容易であるが、逆関数を求めることが計算量的に困難である関数である。つまり、Y=f(X)において、XからYを求めることは容易であるが、逆にYからXを求めることが難しい。

ディフィとヘルマン（W.Diffie、M.E.Hellman）は素数pを法とする有限体（ガロア体GF(p)）におけるべき乗演算に基づく公開鍵暗号方式を提案している。なお、詳細については米国特許No.4,200,770を参照すること。

ディフィとヘルマンの公開鍵暗号方式の基本演算は以下のとおりである。

暗号化: $Y=X^E \mod p$

復号 : $X=Y^D \mod p$

X,YはP以下の整数

ここで、Xは平文、Yは暗号文、Eは秘密の暗号化べ

き、Dは秘密の復号べきである。

ディフィとヘルマン、またはヘルマンとポーリグ（M.E.HellmanとS.C.Pohlig）による（独立にマークルによる）鍵管理システムは2つのフェーズからなる。つまり、まず公開値を交換することによって端末間で秘密のデータを共有して、次にこの共通の秘密値を例えばDESのような慣用鍵暗号方式の鍵として用いてメッセージの暗号化を行なう。なお、ヘルマンとポーリッジの提案した方法については米国特許No.4,124,414に詳しい。

ディフィとヘルマンの提案した公開鍵暗号方式の安全性は、大きな素数pを法とする有限体GF(p)上の離散対数を求める困難さに依存している。素数pを大きくとると、GF(p)上のべき乗演算は一方向性関数と考えることができる。つまり、XとNから、$Y=X^N$ modulo pを求めることは容易であるが、YとXから$N=\log_X(Y)$を求めること、つまり、GF(p)上で離散対数を求めることは計算量的に困難である。pを1000ビットの素数にとると、GF(p)上の離散対数を求めるには、クレイマシンで、現在知られている一番効率的なアルゴリズムを用いても、膨大な時間がかかることが知られている。逆に、暗号化と復号の基本演算であるGF(p)上のべき乗はすぐに求めることができる。

暗号化べきEと復号べきDを、例えばユークリッドの定理を用いて$D\times E=1$ modp-1を満たすように求める。

この条件により、$(X^E)^D=1$ modulo pが成り立ち、pより小さな平文Xを

$Y=X^E$ modulo p

によって暗号化し、

$X=Y^D$ modulo p

よって復号することができる。

ここで、E,Dは秘密に管理され、DからE、またはEからDは簡単に求めることができる。上記2式を満足するp,X,Yから秘密の暗号化べきEあるいは復号べきDを求めることは、GF(p)における離散対数問題を解く困難さに依存して計算量的に困難である。pを512ビットの大きな素数に選ぶと、離散対数問題を解く困難さはDES暗号に対する総当たり攻撃に比べて、何倍もの計算量が必要であると見積ることができる。

以下、ネットワークにおける2つの端末（端末Aと端末Bとする）において、公開値を交換することによって秘密の値を共有できる方法について述べる。基本的なディフィとヘルマンの暗号方式を第5図に示す。この図において各端末における秘密の値は箱の中に示している。秘密の値は決してそのままの形では通信路上に現われない。

まずネットワークで公開の、素数pと0からp-1の任意の整数aを決定する。

（1）端末Aは秘密の値XAを生成し、それに対して公開値

$YA=a^{XA}$ modulo p

を求める。

素数pが大きい場合、公開値YAから秘密の値XAを求めることは実際上不可能である

（2）端末Bは秘密の値XBを生成し、それに対して公開値

$YB=a^{XB}$ modulo p

を求める。

素数pが大きい場合、公開値YBから秘密の値XBを求めることは実際上不可能である。

（3）端末Aは公開値YAを端末Bに、端末Bは公開値YBを端末Aに送信する。交換則により、端末A,Bは

$Z=YB^{XA}$ modulo p

$=(a^{XB}$ modulo $p)^{XA}$ modulo p

$=(a^{XA}$ modulo $p)^{XB}$ modulo p

$=YA^{XB}$ modulo p

を共有することができる。

（4）次に、端末Aと端末Bは、$Z\times Z^*=1$ modulo p-1を満たすZの逆数Z^*を求める。

特に、ディフィとヘルマンの暗号システムにおいては、素数pを

$p=2q+1$　　（q:素数）

を満たすように選ぶ。Zが奇数の場合、Z^*を

$Z^*=Z^{q-1}$ modulo p-1

で求めることができる。もしZが奇数でない場合は、例えば1を加算することによってZを奇数にしてか

らZ'を求める。

共有できた秘密のZ,Z'は端末A、Bの間でメッセージの暗号化／復号に用いられる。つまり、前述した暗号化と復号方式における暗号化べきEをZとし、復号べきDを Z' とする。

なお多くの場合は、端末A、BはZとZ'を用いて慣用鍵暗号のための暗号化鍵を交換する。これは、べき乗演算を用いた暗号化方式が、データの暗号化を行なうには処理が非常に遅いからである。

毎回、端末A、B間の共有鍵を変更するには次の方法がある。まず、端末Aと端末Bはそれぞれ乱数を生成し、これを前述のZとZ'を用いて秘密に交換する。そして2つの乱数系列のビットごとの法2の加算を行ない暗号鍵を求める。

また、もう1つ方法は、端末Aと端末Bが新しい秘密の値と公開値を生成し、公開値を交換して、新しい秘密の共有値Sを求める。これをある関数を用いてもとの秘密の共有値Zと結合して（例えば、M-Z×S modulo p）、秘密の暗号鍵を生成する。

（RSA公開鍵暗号方式）

RSA暗号はリベスト、シャミア、アドルマン（R.Rivest, A.Shamir, L.Adleman）らによって提案された公開鍵暗号方式である。詳細については米国特許No.4,405,829を参照すること。RSA暗号の安全性はある整数を素因数分解する困難さに依存している。ディフィとヘルマンの暗号システムと同様に、暗号化と復号はべき乗演算を用いて行なわれる。しかしながら、RSA暗号システムにおいてはディフィとヘルマンの暗号システムのように法は素数ではない。法は2つの秘密の素数の積であり、安全性を保証するためその値はネットワークにおける各端末ごとに相異なる必要がある。

RSA暗号システムを用いて、以下のとおり端末Aと端末Bは公開値を交換することによって秘密のメッセージを交換することができる。端末Bはまず、2つの大きな秘密の素数pB,qBと、端末Bの秘密の復号べきDB,端末Bの公開の暗号化べきEBを生成する。ただし、EB,DBは、EB×DB-1 modulo (pB-1)(qB-1)を満たす。

なお、Bの秘密の素数を知らないと公開の暗号化べきEBから復号べきDBを求めることはできない。RSAシステムが'強く'なるためには、p-1とq-1も大きな素数の因数をもたなければならない。

端末Aが端末Bに秘密のメッセージを送るためには、まず、受信者端末Bは端末Aに自分の公開値EB、NB(=pB×qB)を通知する。

そして、端末Aはこの端末Bの公開値を用いて次のべき乗計算を行なうことによって、メッセージXを暗号化する。

$$Y=X^{EB} \text{ modulo } NB$$

端末Bだけがこの暗号文を自分の秘密の復号べきを用いて、次のように復号することができる。

$$X=Y^{DB} \text{ modulo } NB$$

さらに、RSA暗号システムを用いて端末Bが公開のメッセージMの署名を生成し、端末Aに認証してもらうことができる。端末Bは自分の秘密の復号べきを用いて、

$$C=M^{DB} \text{ modulo } NB$$

を計算し、メッセージMと共に端末Aに送付する。

端末Aは、端末Bの公開値を用いて、

$$M=C^{EB} \text{ modulo } NB$$

からMを得る。Bの公開値を知っている端末なら誰でもこのCからMを得ることができる。しかし、端末BだけがMからCを作ることができる。

CからMが得られることによって、端末AおよびBの公開鍵を知っている任意の端末は、端末Bが確かにメッセージMを送信したということを認証できる。このように、メッセージMにはこの手続きによって、端末Bの署名を付加することができる。

端末Aも同様に2つの大きな秘密の素数pA,qAと、端末Aの秘密の復号べきDA,端末Aの公開の暗号化べきEAを生成する。但し、EA,DAはEA×DA-1 modulo (pA-1)×(qA-1)を満たす。

以上のRSA暗号システムにおける暗号通信と署名通信を組み合わせて、双方向で秘密の署名付きのメッセージを交換することができる。第6図にその様子を示す。メッセージに自分の秘密鍵で署名を付加し、さらに相手の公開鍵でこれを暗号化して相手に送信する。受信者は送信されたきたデータを自分の秘密鍵で復号し、さらに相手の公開鍵

で署名を取り除いてメッセージを得る。なお、ディフィとヘルマンの暗号方式と同様にRSA暗号システムにおいても、処理が非常に遅いべき乗演算を用いるため、こうして共有したデータは一般に慣用鍵暗号のための鍵として用いられる。

また、RSA暗号においては、各端末ごとに相異なった合成数を法として持たなければならない。一方、ディフィとヘルマンの暗号システムにおいてはネットワーク全体で1つの素数pを決めておき、これを法とする演算を行なえばよく、暗号化と復号の計算が簡単である。

発明が解決しようとする課題

以上述べたように、従来の鍵配送方式には以下の課題がある。

(1) 慣用鍵暗号を用いた鍵配送では、例えばn個の端末間ではn(n-1)/2個の相異なる共有鍵が必要であり、また加えて秘密の通信路が必要であるため、大規模ネットワークには適していない。

(2) ディフィとヘルマンによって提案された鍵配送方式は、システムにおける2つの端末間の直接的な鍵配送が可能である。しかしながら、このプロトコルにおいては有限体上のべき乗演算が必要であり、安全性を確保するためにその次数は大きくしなければならない。高次の有限体上のべき乗演算を実用的な速度で行なうには、専用のハードウェアや高速のDSPが必要である。

(3) RSA暗号システムを用いた鍵配送方式は、暗号通信や署名通信が容易に実現できるが、各端末ごとに法の値が異なるために、計算が煩雑である。また、ディフィとヘルマンによって提案された方式と同様に、高次のべき乗演算が必要であるため、実用的な速度での処理が困難である。

本発明は、上述の課題に鑑みて試されたもので、以下の特徴を持つ暗号鍵配送方式を提供することを目的とする。

(1) 複数の端末が、ネットワークセンターを介して安全な秘密鍵を得る。

(2) ネットワークセンターの鍵管理負担を取り除く。

(3) ハードウェア量に制限のある端末が、実用的な時間内で共有鍵を得る。

(4) 複数の端末間で、共有の秘密鍵を得る。

(5) 自動車電話ネットワークにおいて端末に秘密鍵を配送する。

課題を解決するための手段

前記目的を達成するために、本発明における暗号通信システムは、第1の端末と第2の端末とネットワークセンターより構成され、第1、第2の生成手段、第1、第2の構造化手段、第1、第2、第3の暗号化手段、要求信号生成手段、第1、第2の復号手段、そして正当性確認手段からなる。第1、第2の生成手段は第1、第2の鍵暗号化鍵生成部で実現され、第1、第2の構造化手段は第1、第2の構造化データ部で実現される。また、第1、第2、第3の暗号化手段はそれぞれ第1の公開鍵暗号部、第2の公開鍵暗号部、慣用鍵暗号部で実現される。要求信号生成手段はネットワークセンターか別の装置において実現される。第1、第2の復号手段はそれぞれ公開鍵復号部、慣用鍵復号部で実現され、正当性確認手段は構造化データ確認部で実現される。

また、本発明は、次のようなステップからなる暗号通信方法を含む。

第1の鍵暗号化鍵を生成し、公開鍵暗号アルゴリズムを用いてこれを第1の暗号文に暗号化し、第2の暗号化鍵を生成し、公開鍵暗号アルゴリズムを用いてこれを第2の暗号文に暗号化し、公開鍵復号アルゴリズムを用いて第1、第2の暗号文を復号し、その結果、第1の鍵暗号化鍵と第2の鍵暗号化鍵を得て、慣用鍵暗号を用いて第1の鍵暗号鍵と第2の鍵暗号化鍵を暗号化して第3の暗号文を生成し、慣用鍵復号アルゴリズムと第1の鍵暗号化鍵を用いて第3の暗号文を復号し、第2の鍵暗号化鍵を得る。

作用

第1の鍵暗号化鍵生成部は第1の端末にあり、第1の鍵生成鍵を生成する。第1の構造化部は第1の端末にあり、第1の構造化データを生成する。第1の公開鍵暗号部は第1の端末にあり、第1の鍵暗号化生成部と第1の構造化部と通信路に接続

している。そして、公開鍵暗号アルゴリズムを用いて第1の鍵暗号化鍵と第1の構造化データを暗号化して第1の暗号文を生成し、通信路に送信する。

ネットワークセンターは、第1の暗号文を受け取ると要求信号を生成し、通信路を通して第2の端末にこれを送信する。

第2の端末ではこの要求信号を受け取ると、第2の鍵暗号化鍵生成部において第2の鍵暗号化鍵を生成し、第2の構造化部において第2の構造化データを生成する。第2の公開鍵暗号部は第2の鍵暗号化鍵生成部と第2の構造化部と通信路に接続しており、公開鍵暗号アルゴリズムを用いて第2の鍵暗号化鍵と第2の構造化データを暗号化して第2の暗号文を生成し、通信路に送信する。

ネットワークセンターでは、通信路に接続している公開鍵復号部が、公開鍵復号アルゴリズムを用いて第1の暗号文と第2の暗号文を復号する。この結果、ネットワークセンターは第1の鍵暗号化鍵と第1の構造化データ、第2の鍵暗号化鍵と第2の構造化データを得る。

ネットワークセンターにある構造化データ確認部は公開鍵復号部に接続しており、第1の構造化データと第2の構造化データの正当性を確認して正当性確認信号を生成する。慣用鍵暗号部は、ネットワークセンターにあり、構造化データ確認部公開鍵復号部と通信路に接続している。そして正当性確認信号を受け取ると慣用鍵暗号アルゴリズムを用いて第1の鍵暗号化鍵と第2の鍵暗号化鍵を暗号化し、第3の暗号文を生成し、通信路に送信する。

慣用鍵復号部は、第1の端末にあり、通信路に接続している。そして慣用鍵復号アルゴリズムと第1の鍵暗号化鍵を用いて第3の暗号文を復号する。この結果、第1の端末は第2の鍵暗号化鍵を得る。

実施例

第1図は本発明の第1の実施例における暗号通信システムの構成を示すブロック図を示すものである。

第1図に示すとおり、本実施例は第1の端末20、第2の端末40、ネットワークセンター30より構成される。第1の端末20は第1の鍵暗号化鍵生成部24、第1の公開鍵暗号部22、慣用鍵復号部26で構成される。第1の鍵暗号化鍵生成部24は第1の公開鍵暗号部22に接続している。また、第1の公開鍵暗号部22と慣用鍵復号部26は通信路に接続している。ネットワークセンター30は慣用鍵暗号部34、公開鍵復号部32からなる。公開鍵復号部32と慣用鍵暗号部34は接続され、また双方は通信路に接続されている。第2の端末40は第2の鍵暗号化鍵生成部44、第2の公開鍵暗号部42からなる。第2の鍵暗号化鍵生成部44は公開鍵暗号部42に接続され、公開鍵暗号部42は通信路と接続されている。

以上のように構成された第1の実施例の動作を以下に説明する。

第1の公開鍵暗号部22では鍵暗号化鍵生成部24で生成された鍵暗号化鍵r1を、公開鍵暗号アルゴリズムを用いて、第1の暗号文に暗号化する。第1の公開鍵暗号部22はこれを通信路に送信する。

ネットワークセンター30はこの第1の暗号文を受け取ると、要求信号を生成し、通信路を用いて第2の端末40に送信する。

第2の端末40ではこの要求信号を受け取ると、第2の鍵暗号化鍵生成部44において第2の鍵暗号化鍵信号r2を生成する。第2の公開鍵暗号部42は公開鍵暗号アルゴリズムを用いて第2の鍵暗号化鍵r2を、第2の暗号文に暗号化する。そしてこれを通信路を介してネットワークセンター30に送信する。

ネットワークセンター30にある公開鍵復号部32は公開鍵復号アルゴリズムを用いて第1、第2の暗号文を復号する。この結果としてネットワークセンター30は第1の鍵暗号化鍵r1と第2の鍵暗号化鍵r2を得る。

慣用鍵暗号部34は慣用鍵暗号アルゴリズムを用いて第1の鍵暗号化鍵と第2の鍵暗号化鍵を第3の暗号文に暗号化する。そしてこれを通信路を

介して第1の端末20に送信する。

第1の端末20にある慣用鍵復号部26では、第1の鍵暗号化鍵r1を用いて第1の暗号文を復号する。この結果、第1の端末は第2の鍵暗号化鍵を得る。ここで、第1の端末20と第2の端末40は第2の鍵暗号化鍵を共有できた。そしてこれを任意の標準暗号アルゴリズムの鍵として用いればよい。

また、第1の鍵暗号化鍵r1を秘密に共有する場合は、第3の暗号文が通信路を介して第2の端末40に送信される。第2の端末40では、慣用鍵復号部が慣用鍵復号アルゴリズムと第2の鍵暗号化鍵r2を用いて第3の暗号文を復号し、第1の鍵暗号化鍵r1を得る。

本発明においては端末からネットワークセンターへの通信には公開鍵暗号系を用いる。このことより、それぞれの端末はネットワークセンターの公開鍵だけを保管していればよい。また、公開鍵暗号は一般に少ない計算量で実現可能であるため、ハードウェア量に制限のある端末でもこの処理は実用的な時間内でできる。

第2図は本発明の第2の実施例における暗号通信システムの構成を示すブロック図を示すものである。第2図に示すとおり、第2の実施例は第1の実施例における第1の端末20に、第1の構造化部28を追加している。第1の構造化部は第1の公開鍵暗号部22に接続する。同様に、第2の端末40に第2の構造化部48を追加し、これは第2の公開鍵暗号部42に接続している。さらにネットワークセンター30に構造化データ確認部36を追加する。これは慣用鍵暗号部34と公開鍵復号部32に接続している。第1の鍵暗号化鍵生成部24は第1の端末20にあり、第1の鍵暗号鍵を生成する。第1の公開鍵暗号部22は第1の端末にあり、第1の鍵暗号化鍵生成部24と通信チャネルに接続している。通信路は第1の端末20とネットワークセンター30の間、そして第2の端末40とネットワークセンター30の間を結ぶ。

以上のように構成された第2の実施例の動作を以下に説明する。第2図に示すとおり、第2の実施例では、第1、第2の構造化手段とその正当性確認手段を含んでいる。

第1の構造化部28と第2の構造化部48は、例えばタイムスタンプや識別情報または、任意のタイプのデータ構造を導入する。

第1の公開鍵暗号部22は第1の鍵暗号化鍵と第1のデータ構造化部28で生成された第1の構造化データを、公開鍵暗号アルゴリズムを用いて第1の暗号文に暗号化する。ネットワークセンター30の公開鍵復号部32は第1の暗号文を復号し、第1の構造化データと第1の鍵暗号化鍵を得る。データ構造化確認部26では、第1の構造化データがデータのあらかじめ定めた構造を持つか否かを確認する。例えば、もし構造化データがタイムスタンプを含んでいた場合、データ構造化確認部36はタイムスタンプで示された時間が妥当であるかを確認する。

同様に、第2の端末は要求信号を受け取り、第2のデータ構造化部48で第2の構造化データを生成する。第2の公開鍵暗号部42は第2の鍵暗号化鍵と第2の構造化データを、公開鍵暗号アルゴリズムを用いて第2の暗号文に暗号化する。ネットワークセンター30の公開鍵復号部32は第2の暗号文を復号し、第2の鍵暗号化鍵と第2の構造化データを得る。

データ構造化確認部36では、第2の構造化データがデータのあらかじめ定めた構造を持つか否かを確認する。

次に、第1、第2の実施例の動作をより具体的に説明する。説明のため、公開鍵暗号系としてRSA暗号を用いる。法nは素数p,qの積である。暗号化べきeは3に選ぶ。復号べきdはe×d=1 modulo Lを満たす数である。なお、ここでL=LCM(p-1,q-1)である。

また慣用鍵暗号系としては簡単な換字暗号を考える。簡単な換字暗号の1つの例としてバーナム暗号がある。その暗号化と復号は以下のとおりである。

暗号化: E(x,k)=x○k

復号: D(x,k)=x○k

ここで、○はビットごとの法2の加算を示す。

また、他の例としては以下で示す法nの加算がある。

暗号化: E(x,k)=x+k modulo n

復号: D(x,k)=x+k modulo n

ここで、x,kはnを法とする剰余環上の任意の要素である。

まず、第1の実施例について具体的に述べる。

鍵配送プロトコル1(KDP1)

1.第1の端末が鍵暗号化鍵としてr1を生成する。

2.第1の端末はネットワークセンターの公開鍵(e=3)を用いてr1を暗号化する。そしてr1^e modulo nをネットワークセンターに送信する。

3.ネットワークセンターはr1^e modulo nをその秘密鍵dで復号して

(r1^e modulo n)^d modulo n=r1を得る。

4.ネットワークセンターは第2の端末を呼び出す。

5.第2の端末は第1の端末と第2の端末間のセッション鍵としてr2を生成する。

6.第2の端末はネットワークセンターの公開鍵(e=3)を用いてr2を暗号化する。そしてr2^e modulo nをネットワークセンターに送信する。

7.ネットワークセンターはr2^e modulo nをその秘密鍵dで復号して

(r2^e modulo n)^d modulo n=r2を得る。

8.ネットワークセンターは慣用鍵暗号E( )を用い鍵暗号化鍵r1でr2を暗号化して第1の端末にE(r2,r1)を送信する。

9.第1の端末は自分の生成した鍵暗号化鍵r1でE(r2,r1)を復号する。そしてD(E(r2,r1),r1)=r2を第2の端末との共有のセッション鍵として得る。

KDP1における端末の計算は、慣用鍵暗号方式として前述の換字暗号を用いるとき、べき数3のべき乗剰余演算と、ビットごとの法2の加算または法nの加減算だけである。従って、ハードウェア量が制限されている端末でも容易に実現できる。

次に、慣用鍵暗号として法n上の加算を用いた場合の安全性について述べる。

まず、通信路上に現われる、r1^3 modulo n とr2^3 modulo n、r1+r2 modulo n だけを用いて行なう受動的攻撃に対しては安全性が劣化しないことを以下に示す。

通信路上の暗号文を盗聴することによって解読者は以下のa,b,cを得る。

$$r1^3=a \quad \text{modulo } n \qquad (1)$$

$$r2^3=b \quad \text{modulo } n \qquad (2)$$

$$r1+r2=c \quad \text{modulo } n \qquad (3)$$

これらの関係式から解読者は以下の法n上のr1の2次方程式を得る。

$$r1^2-c\times r1+(1/3c)(c^3-a-b)=0 \quad \text{modulo } n \qquad (4)$$

但し、ここでGCD(3c,n)=1とする。

ラビン(Rabin)はnの素因数を知らずに(4)の2次方程式をとくことは、n=pqを素因数分解する困難さと同等に難しいことを示している。一方、RSA暗号の安全性はnの素因数分解に依存して困難であるとされている。従って、このプロトコルにおいてr1+r2 modulo n が通信路上に表れても、プロトコルの安全性は劣化しない。

次に、解読者がこの鍵配送プロトコルに参加して行なう能動的攻撃に対しての、KDP1の安全性について述べる。

KDP1は能動的攻撃に対して、弱点があることが示されている。攻撃には2種類あり、以下、その攻撃法についてそれぞれ説明する。

双方の攻撃法では、第1、第2の解読者が結託してプロトコルに参加し、それ以前に配送された正規の第1、第2の端末の共有鍵を得ることができる。

そのため、まず第1、第2の解読者はあらかじめ値Rを決めておく。

まず、第1の攻撃では、第1の解読者が、第2の解読者との鍵共有を要求して、正規の第1の端末からネットワークセンターへの送信を盗聴して得たデータr1^3 modulo n を再送する。第2の端末はあらかじめ決めておいた数Rを公開鍵暗号を用いて暗号化してネットワークセンターに送信する。ネットワークセンターでは第1、第2の解読者からの暗号文を復号して得たr1,Rを、慣用鍵暗号方式を用いて暗号化して第1の解読者に送信する。第1の解読者はこの暗号文をRで復号することによ

り明らかにr1、さらに正規の第1、第2の端末の共有鍵r2を得ることができる。従って、KDP1の方法は再送攻撃に対して弱い。

次に述べる第2の攻撃では、ネットワークセンターがなりすまし攻撃に対する防御メカニズムをもっていたとしても、解読者が防御メカニズムを回避して共有鍵r2を得ることができる。

KDP1に対する解読方法

1.第1の解読者は乱数r3を選び、その逆数$r3^{-1}$ modulo nを計算する。盗聴データa=$r1^e$ modulo nを用いて、$a\times r3^e=r1^e\times r3^e$ modulo nを計算し、第2の解読者との鍵共有を要求してネットワークセンターにこれを配送する。

2.ネットワークセンターは$r1^e\times r3^e$ modulo nを復号してr1×r3 modulo nを得る。

3.ネットワークセンターは第2の解読者を呼び出す。

4.第2の解読者はあらかじめ第1の解読者と決めておいたRを用いてR^e modulo nを計算し、ネットワークセンターに送信する。

5.ネットワークセンターはR^e modulo nを復号してRを得る。

そして、R+r1×r3 modulo nを計算して第1の解読者に送る。

6.第1の解読者はこれからRを引き、$r3^{-1}$ modulo nを乗してr1を得る。

7.第1の解読者は、盗聴データc=r1+r2 modulo nからr1を減算することによってr2を得る。なお、r2は第1、第2の端末間の共有鍵である。

r3はセンターにとって未知であり、r1×r3 modulo nは1回限りの鍵となるため、第1の解読者はこの中にr1が含まれていることを隠して、ネットワークセンターの再送防止メカニズムを回避することができる。この攻撃は、RSA暗号における分配則$r1^e\times r3^e=(r1\times r3)^e$を利用している。

前記攻撃に対する1つの対策は、第1の鍵暗号化鍵に構造化を付加することである。

RSA暗号の乗法的な性質を使って行なう攻撃を防ぐため、暗号化するデータにあるあらかじめ定めた構造を導入する。例えば512ビットのデータのうち後半256ビットに意味のあるデータを格納し、前半256ビットを必ずゼロにするようなデータ構造が考えられる。センターは復号したメッセージがこのあらかじめ定めた構造をもっているかをチェックする。あらかじめ決められた構造をもつデータの集合をMとする。もしデータr1,r3がMに含まれる要素であるとき、r1×r3 modulo nがMに含まれる確率は非常に小さい。従って、上記の攻撃において、センターは解読者から受け取った$r1^e\times r3^e$ modulo nが不正なデータであることを、高い確率で検出することができる。

再送を防ぐ別の方法は、第1の端末がタイムスタンプを生成し、これを第1の鍵暗号化鍵に結合して暗号化し、送信するという方法である。従って、第1の端末からセンターに送信するデータは、

$(t1||r1)^e$ modulo n

となる。ここで、t1はタイムスタンプ、||はデータの結合、r1は乱数を示す。

センターはタイムスタンプにより時刻の正当性を確認する。タイムスタンプには送信の日付、時間、有効期限を含めることができる。

なりすまし攻撃を防ぐまた別の方法は端末認証である。これは前記述べた能動的攻撃に対する防御法とは直接は関係がないが、備えられるべき機能である。

本発明の鍵配送方式に有効な端末認証方式について述べる。

ネットワークセンターは端末1の秘密s1を端末1の識別情報ID1を用いて、

s1=f(ID1)

で求める。ここでfはセンターだけが知っている多項式関数である。ネットワークセンターはこのs1を、例えばスマートカードに格納して端末1に秘密に配送する。

第1の端末1は自身の秘密情報s1、乱数r1、その他の情報を結合してデータを構成し、これを暗号化する。ネットワークセンターではこの暗号文を復号して端末1の秘密情報s1'を得る。一方ネットワークセンターは端末1の識別情報ID1を用いてf(ID1)を計算して、s1を求めて受け取ったs1'と比

較する。もし一致すればネットワークセンターは送信者を認証する。そうでなければセンターは送信者を拒絶して鍵配送プロトコルを終了する。

これら3つのメカニズムを結合すると、第2の実施例で示している鍵配送方式となる。

鍵配送方式2(KDP2)

1.第1の端末は鍵暗号化鍵としてr1を生成する。

2.第1の端末はネットワークセンターにID1,(t1||s1||r1)^e modulo nを送信する。ここでeはネットワークセンターの公開鍵でe-3とする。

3.ネットワークセンターは自身の秘密鍵を用いてこの暗号文を復号し、(t1||s1||r1)を得る。そしてこれからt1,s1,r1をとりだす。ネットワークセンターはタイムスタンプt1の妥当性をチェックし、また、s1-f(ID1)が成り立つことにより第1の端末の正当性を確かめる。

4.ネットワークセンターは第2の端末2を呼び出す。

5.第2の端末は第1、第2の端末間のセッション鍵としてr2を生成する。

6.第2の端末はネットワークセンターにID2,(t2||s2||r2)^e modulo nを送信する。(e-3)

7.ネットワークセンターはこの暗号文を復号して、(t2||s2||r2)を得る。そしてこれからt2,s2,r2をとりだす。ネットワークセンターはタイムスタンプt2の妥当性をチェックし、また、s2-f(ID2)が成り立つことにより第2の端末の正当性を確かめる。

8.ネットワークセンターは、鍵暗号化鍵r1で第2の端末から得たセッション鍵r2を、慣用鍵暗号方式を用いて暗号化する。その結果のr1+r2 modulo nを第1の端末に送信する。

9.第1の端末はこれよりr1を減算し、第2の端末とのセッション鍵としてr2を得る。

このプロトコルでは、送信するデータにあらかじめ決められた構造を導入することによってRSA暗号の分配則を利用した攻撃を防いでいる。タイムスタンプにより再送攻撃を、そして端末認証機能によりなりすまし攻撃を防いでいる。

次に、KDP2の安全性について述べる。このプロトコルでは、第1の端末は通信路上より(t2||s2||r2)^e modulo nそして、端末2と共有のセッション鍵r2を得ることができる。また、送信した時刻からタイムスタンプt2を予測することができる。もし、これらの情報から第2の端末の秘密情報s2を得ることができたら、この暗号系は安全でないことになる。しかしこの問題は一般的に平文の一部が解読者にわかっている場合に平文全体を知る問題になり、現時点で成功した攻撃は報告されていない。

第3図は本発明を複数の端末に拡張した場合について示している。ネットワークセンター30は第1の端末20と第2の端末40と第3の端末60と第4の端末70他の端末と接続されている。各端末はそれぞれ公開鍵暗号部、鍵暗号化鍵生成部、慣用鍵復号部、データ構造化部からなる。前記述べたように、第1の端末にある第1の鍵暗号化鍵生成部が第1の鍵暗号化鍵を生成する。第1の端末にある第1の公開鍵暗号部が第1の鍵暗号化鍵を暗号化して第1の暗号文にする。そしてこれを通信路を介してネットワークセンターに送信する。ネットワークセンター30は第1の暗号文を受け取ると、要求信号を生成し、通信路を介して複数の端末にこの信号を送信する。複数の端末とは第3図にある第2の端末40、第3の端末60、第4の端末70のことである。

各端末では、要求信号を受けて端末内の鍵暗号化鍵生成部でそれぞれ鍵暗号化鍵を生成する。それぞれの鍵暗号化鍵生成部に接続している公開鍵暗号部で、公開鍵暗号アルゴリズムを用いてそれぞれの鍵暗号化鍵を暗号化し、それぞれ通信路を介してネットワークセンター30に送信する。

ネットワークセンター30では、公開鍵復号部で公開鍵復号アルゴリズムを用いて複数の暗号文を復号する。この結果、ネットワークセンター30は第1の鍵暗号化鍵と複数の鍵暗号化鍵を得る。

ネットワークセンター30の慣用鍵暗号部では、慣用鍵暗号アルゴリズムを用いて第1の鍵暗号化鍵と複数の各鍵暗号化鍵を入力として、それぞれの暗号文に暗号化する。そしてこれらを通信路を介してそれぞれの端末に送信する。

各複数の端末においては、慣用鍵復号アルゴリズムとそれぞれ自分の生成した鍵暗号化鍵を用いて、第1の端末が生成した第1の鍵暗号鍵を得る。そしてこの第1の鍵暗号鍵を複数端末間で行なう任意の標準暗号アルゴリズムの鍵として用いることができる。

このように、本発明は自動車電話ネットワークに代表されるスター型ネットワークに適した鍵配送を実現できる。

発明の効果

以上説明したように、本発明によれば、以下に記載されるような効果を奏する。

(1) 複数の端末がネットワークセンターを介して公開の情報を送りあうことにより、安全に秘密鍵を配送する。この通信形態には、例えば自動車電話ネットワークがある。

(2) 端末からネットワークセンターへの通信は、公開鍵暗号方式を用いているため、各端末はネットワークセンターの公開鍵のみを保持してればよい。また、特に公開鍵暗号として小さな暗号化べきをもつRSA暗号を用いると、ハードウェア量に制限のある端末でも実用的な時間内で鍵を共有することが可能となる。

(3) ネットワークセンターから端末への通信は、慣用鍵暗号方式を用いている。この時のネットワークセンターと端末間の共有鍵は、端末から前記公開鍵暗号で送られた情報である。従って、ネットワークセンターは各端末の鍵管理から解放される。特に慣用鍵暗号として簡単な換字暗号、例えば法2の加算やmodulo nの加算を用いると、(2)と同様に鍵共有までの処理時間が短縮できる。

(4) さらに、RSA暗号における分配則に基づいた攻撃を回避するため、送信データにあらかじめ決められたある構造化を取り入れる。また、再送防止のためにタイムスタンプの導入、そしてなりすまし攻撃の防止のために識別情報に基づく端末認証方式も提案している。

(5) また、3端末以上の鍵配送方式にも簡単に拡張できる。

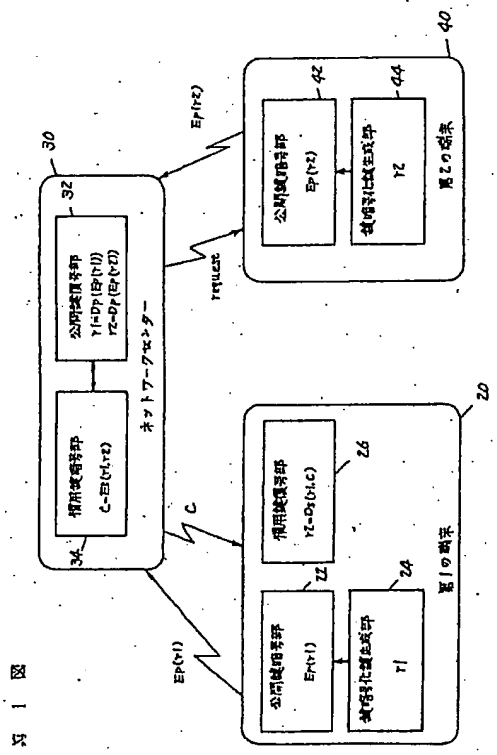
4. 図面の簡単な説明

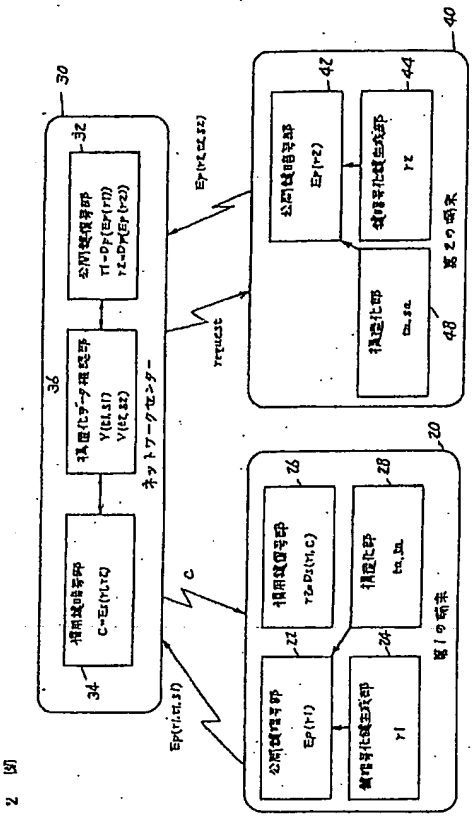
第1図は、本発明における暗号通信システムの構成図、第2図は構造化部を有する暗号通信システムの構成図、第3図は本発明を複数の端末で用いる場合の暗号通信システムの構成図、第4図は慣用鍵暗号システムの構成図、第5図はディフィとヘルマンの公開鍵暗号システム、第6図はRSA暗号システムの構成図である。

20・・・第1の端末、22・・・公開鍵暗号部、24・・・鍵暗号化鍵生成部、26・・・慣用鍵復号部、28・・・構造化部、30・・・ネットワークセンター、32・・・公開鍵復号部、34・・・慣用鍵暗号部、36・・・構造化データ確認部、40・・・第2の端末、42・・・公開鍵暗号部、44・・・鍵暗号化鍵生成部、46・・・慣用鍵復号部、48・・・構造化部。

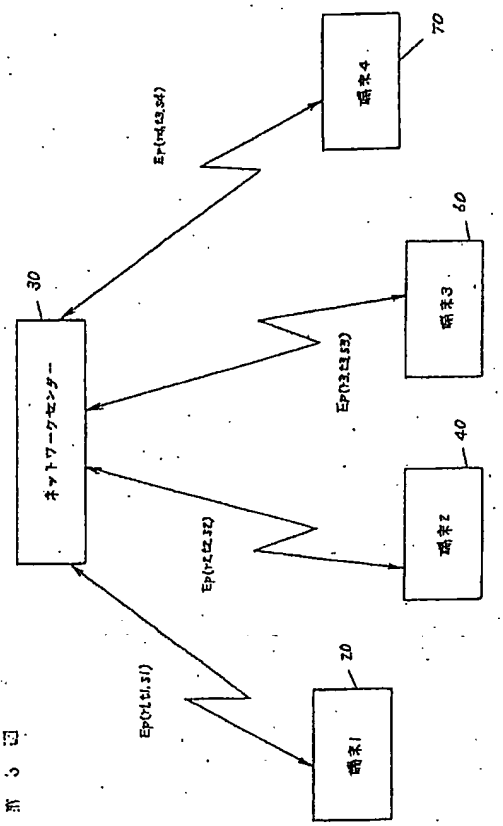
代理人の氏名　弁理士　栗野重孝　ほか1名

第1図



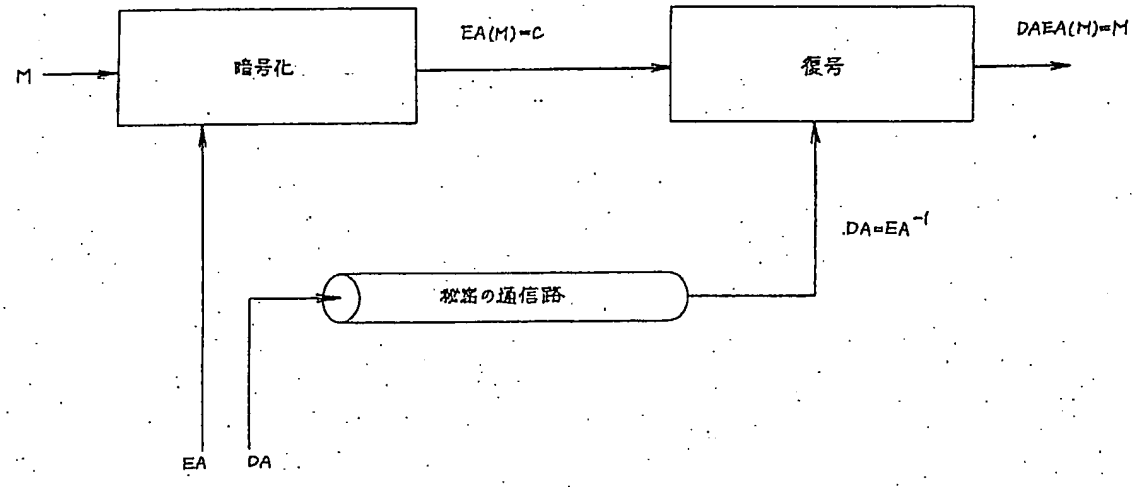

30
32
公開鍵復号部
T1=Dp(Ep(T1))
T2=Dp(Ep(T2))
36
秘匿化データ復号部
Y(t1,s1)
V(t2,s2)
34
相関鍵生成部
C=E(Y,V)
ネットワークセンター
Ep(Y,t1,s1)
request
C
40
42
公開鍵復号部
Ep(T2)
44
秘匿署名生成部
T2
48
秘匿化部
Ep,Sp
第2の端末
20
26
相関鍵復号部
T2=Dp(Y,C)
28
秘匿化部
Ep,Sp
22
公開鍵復号部
Ep(T1)
24
秘匿署名生成部
T1
第1の端末

第2図

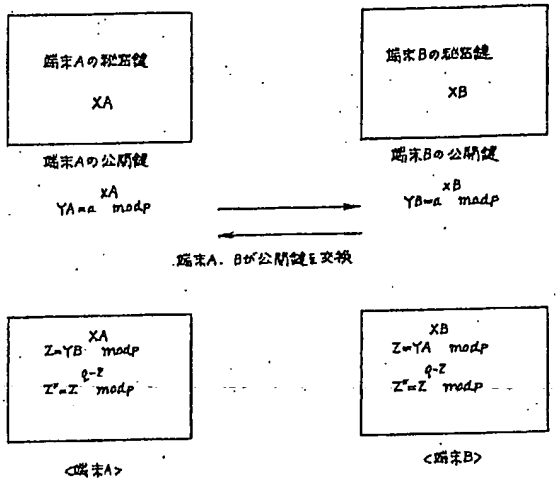

70
端末4
Ep(t4,s4)
60
端末3
Ep(t3,s3)
30
ネットワークセンター
40
端末2
Ep(t2,s2)
Ep(t1,s1)
20
端末1

第3図

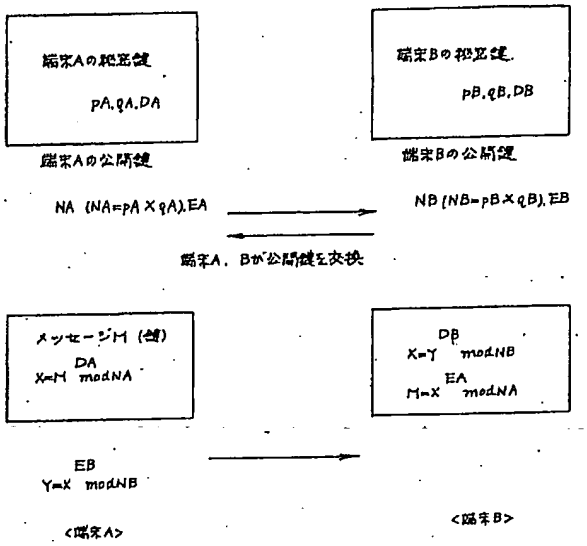
第4図


M
暗号化
EA(M)=C
復号
DAEA(M)=M
DA=EA⁻¹
秘密の通信路
EA
DA

第 5 図


端末Aの秘密鍵
XA
端末Aの公開鍵
YA=a^xA mod p
端末Bの秘密鍵
XB
端末Bの公開鍵
YB=a^xB mod p
端末A，Bが公開鍵を交換
Z=YB^XA mod p
Z'=Z^(q-z) mod p
Z=YA^XB mod p
Z'=Z^(q-z) mod p
<端末A>
<端末B>

第 6 図


端末Aの秘密鍵
pA, qA, DA
端末Aの公開鍵
NA (NA=pA×qA), EA
端末Bの秘密鍵
pB, qB, DB
端末Bの公開鍵
NB (NB=pB×qB), EB
端末A，Bが公開鍵を交換
メッセージM (整)
DA
X=M^DA mod NA
EB
Y=X^EB mod NB
DB
X=Y^DB mod NB
EA
M=X^EA mod NA
<端末A>
<端末B>